REMARKS

Claims 19 and 21-36 are pending in the application. Applicants have not amended the claims by this Amendment. Applicants respond specifically to the issues raised in the Final Office Action mailed on March 8, 2006 as follows:

Claim Rejections -- 35 USC § 103

Claims 19 and 21-36 have been rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 4,629,872 to Hällberg ("Hällberg") in view of U.S. Patent No. 5,882,463 to Tompkin et al. ("Tompkin").

The Hällberg Patent

Hällberg discloses a method for producing and verifying an identification document, which is illustrated in Fig. 1. A personal card or account number PAN, which may be registered in machine-readable code such as a magnetic strip when the card is made (col. 2, lines 19-23), is used as input parameters of an encryption algorithm (col. 2, lines 23 to 27) with a key formed from a secret key number K1 and a pin number PIN. The output is subsequently decrypted by means of a decryption algorithm that uses as key a further secret key number K2 combined with a permanent number FN. The output of the decryption algorithm, the personal check number PCN, is coded into the card in connection with issuing the card (col. 2, lines 27 to 34).

Hällberg teaches that the verification procedure is carried out each time a card owner identifies himself at a terminal as illustrated in Fig. 2. First, the PAN (which can be encoded on

the card) is encrypted with a relation between the secret key number K1 and the PIN entered by the card owner. The PCN (that can be coded into the card) is then encrypted with a relation between the permanent number FN and the secret key number K2. The outputs of the two algorithms are compared and, if they are the same, the card is approved.

In contrast to the method taught by Hällberg, claim 19 of the present application is directed to a method, wherein at least two parameters (the machine-readable document number (DN) and the identification (ID) that is optically read out of optical diffraction structures of an optical marking) are used in a cryptographical operation with a first secret key to produce the check number.

Although Hällberg discloses a machine-readable identification (i.e., PAN -- the card number or account number), Hällberg's secret key number K1 and PIN are not the same as the "at least two parameters" (i.e., the document number (DN) and the identification (ID)) in claim 19. Neither Hällberg's secret key number K1 nor the PIN represents the document number. K1 is a secret key number and PIN is a personal identification number for a user, not the document. Moreover, neither of these two parameters (K1 or PIN) is encoded in the card in machine-readable form. The PIN is a code that has to be kept secret by the card owner. Storing the PIN code in machine-readable form on the card would contradict the basic concept of PIN codes. A PIN code provide security by preventing an unauthorized user in possession of the card form using the card since the PIN code is known only to the card owner and is not stored on the card. The card owner uses the PIN code solely for identification purposes.

Hällberg's secret key number K1 is not encoded in machine-readable form on the card. The secret key number K1 represents a "secret key," i.e., a key that has to be kept secret to prevent unauthorized production of identification documents. "[T]he PAN is encrypted with a relation of a secret key number K1 with the PIN as key to the algorithm" (col. 2, lines 24-26) to produce the personal check number (PCN). If the secret key number K1 is encoded on an issued card, it is no longer secret since the code can be broken to reveal the secret key number. This would allow unauthorized cards to be fraudulently produced. Accordingly, one skilled in the art would understand that Hällberg teaches away from storing the pin number PIN or the secret key number K1 in machine-readable form on the card.

A Comparison of Claim 19 and the Hällberg Patent

The Examiner found at pages 4-5 of the Office Action that Hällberg discloses a method and apparatus for verifying personal identification information using a machine readable code or magnetic strip.

Claim 19 of the present invention is reproduced below with abbreviations for the relevant parameters added and shown in bold faced font and brackets:

> 19. A method of using an activatable document with an at least machine-readable document number **[DN]**, an optical marking with a machine-readable identification **[ID]** and a storage field disposed on a substrate for receiving an at least machine-readable check number **[CN]**, wherein
>
> to complete the document to provide an authenticity certificate the check number **[CN]** is produced as the result of a cryptographic operation [⊙] with at

least two parameters, the document number **[DN]** and the identification **[ID]**, wherein the identification is optically read out of optical-diffraction structures of the optical marking, and a first secret key **[K1]**, only when the document is put into circulation, and is written into the storage field, and

that after the document is put into circulation the authenticity **[A]** of the authenticity certificate is checked by means of the check number **[CN]** read out of the storage field and at least the parameters **[DN and ID]** read on the authenticity certificate of the cryptographic operation [⊙] by means of a second key **[K2]** different from the first key.

Claim 19 discloses a two-step process with the first step disclosed in the second paragraph and the second step disclosed in the third paragraph. In the first step, a document is provided with a authenticity certificate in the form of a check number **[CN],** which is produced using a cryptographic operation **[⊙]** that includes at least two parameters (the document number and the identification -- **[DN and ID])** and a first secret key **[K1]**. The first step is illustrated by the following formula:

$$(ID + DN) \odot K1 = CN \qquad (1)$$

wherein K1 is a first secret key and ⊙ is a first cryptographic operation.

In the second step, the authenticity **[A]** of the document is checked using the check number **[CN]** and at least two parameters **[DN and ID]** and a second secret key **[K2]**. The second step can be illustrated by the following formula:

$$[CN + (ID + DN)] \text{ ⊙⊙ } K2 = A \qquad (2)$$

wherein K2 is a second secret key and ⊙⊙ is a second cryptographic operation.

Thus, in claim 19, a first cryptographic operation is used to produce the check number **[CN]** and a second cryptographic operation is used to authenticate the check number **[CN]**. In both steps, the secret keys have a corresponding algorithm.

In contrast to claim 19, Hällberg teaches a two step process to produce a personal check number **(PCN)**. Fig. 1 of Hällberg illustrates how in a first step a personal account number **(PAN)** is "encrypted [⊙] with a relation of a secret key number **K1** with the **PIN** as key to the algorithm." Col. 2, lines 24-26. After the first encryption, in step 2, the code encrypted in step 1 is decrypted [⊙⊙] by "an algorithm with a relation between the permanent number **FN** and a secret key number **K2** as the key to the algorithm." Col. 2, lines 27-30.

Hällberg's two-step process for creating the personal check number **(PCN)** can be illustrated by the following formula:

$$[PAN \text{ ⊙ } (PIN \text{ ® } K1)] \text{ ⊙⊙ } (FN \text{ ® } K2) = PCN \qquad (3)$$

wherein ® is a relation, ⊙ is an encryption and ⊙⊙ is a decryption.

Fig. 2 of Hällberg illustrates how the **PCN** is verified. First, "the **PAN** is algorithm encrypted with a relation between the secret key number **K1** and the **PIN** as key." Col. 2, lines 42-44. Then, "the **PCN** is algorithm encrypted with the relation between the permanent number

FN and the secret key number **K2** as key." Col. 2, lines 45-48. "The out puts of the two algorithms are compared, and if these are the same, then so is the identification." Col. 2, lines 49-50. Hällberg's verification process is performed by the following comparison:

$$PAN \text{ ⊙ } (PIN \text{ ® } K1) \quad = \text{or} \neq \quad PCN \text{ ⊙ } (FN \text{ ® } K2) \qquad (4)$$

wherein ® is a relation and ⊙ is an encryption.

The present invention and Hällberg produce and verify check numbers using different methods. A comparison of claim 19 (formula (1)) and Hällberg (formula (3)) shows that even though both methods perform encryptions, they are substantially different. Claim 19 produces a check number **[PCN]** on a document as shown in formula (1) using a cryptographic operation [⊙] that includes at least two parameters **[DN and ID]** and a secret key **[K1]**. In contrast, Hällberg produces a check number **[PCN]** on a document as shown in formula (3) using a two-step encryption and decryption operation that includes a personal account number **[PAN]**, a first secret key number **[K1]**, a personal identification number **[PIN]**, a permanent number **[FN]** and a second secret key number **[K2]**. Thus, the method in claim 19 is a one-step encryption that requires only two parameters **[DN and ID]** and a secret key **[K1]**, while the method in Hällberg is a two-step encryption/decryption that requires three parameters (**PAN**, **PIN** and **FN**) and two secret keys (**K1** and **K2**).

Similarly, claim 19 authenticates a check number **[PCN]** on a document as shown in formula (2) using a cryptographic operation [⊙⊙] that includes the check number **[CN]** and at

least two parameters **[DN and ID]** and a second secret key **[K2]**. In contrast, Hällberg authenticates a check number **(PCN)** on a document as shown in formula (4) by comparing the results of two encryptions using algorithms. In the first encryption, a personal account number **(PAN)** is encrypted with a relation between a personal identification number **(PIN)** and a first secret key **(K1)**. In the second encryption, a personal check number **(PCN)** is encrypted with a relation between a permanent number **(FN)** and a second secret key **(K2)**. Thus, the authentication method in claim 19 is a single cryptographic operation that includes the check number **[CN]** and requires only two parameters **[DN and ID]** and a secret key **[K2]**, while Hällberg's authentication method requires two algorithm encryptions, wherein the **PAN** is encrypted by a relation between the **PIN** and a first secret key **K1** and the **PCN** is encrypted by a relation between the **FN** and a second secret key **(K2)**. If the outputs of the two algorithms are equal, the authenticity of the **PCN** is verified.

The Tompkin Patent

The Examiner also found at page 4, lines 15-17 of the Office Action that:

> Hällberg does not explicitly disclose the identification is optically read out of optical-diffraction structures of the optical marking.

The Examiner has cited Tompkin to cure this deficiency. However, Tompkin does not teach nor suggest the method of producing and authenticating a check number as disclosed in claim 19 and, thus, Tompkin does not overcome the deficiencies in the teachings of Hällberg discussed in the preceding sections.

The Present Invention Is Not Obvious In View Of A Combination Of Hällberg And Tompkin.

Neither Hällberg nor Tompkin teaches reading the identification (which is used together with the document number as input parameters of the cryptographical operation) out of optical diffraction structures of an optical marking. Optical diffraction structures containing machine-readable information provide a high level of safeguard against forgery and copying. However, from a practical point of view, such optical diffraction structures can be manufactured in a cost-efficient manner only when produced in great quantities. An embossing dye has to be provided for each diffractive structure that is incorporated in the document. This is expensive and only cost-efficient if the embossing dye is used for a large number of documents.

The present invention uses two different types of information as input parameters for the cryptographical operation that is used to produce the check number stored on the document during the activation process. The first type of information is the machine-readable document number which uniquely identifies the document, but which can easily be falsified and copied. The second type of information is the machine-readable identification read out of the optical diffraction structures of the optical marking. This information is difficult to falsify and copy, but it is also hard to individualize and must be manufactured in large series in order to be cost-efficient. Combining the two different parameters by means of the asymmetric cryptographical operation improves the safeguard against forgery or falsification while still enabling cost-efficient manufacture of the card since the document-number already provides information uniquely identifying the document (see specification, page 3. lines 22-26).

The Examiner's Findings

At page 3, line 17 - page 4, line 3 and page 4, lines 15-17 of the Office Action, the examiner states:

> Hallberg discloses a check number (PCN) produced as a result of cryptographic operation; Hallberg discloses a card number or account number (PAN) in machine readable code or magnetic strip that meets the recitation of identification, and a first secret key producing the check number by cryptographic operation with at least two parameters (secret key number and a PIN) when issuing the card (column 2, lines 16-45) and the check number is written to a storage field disposed on a substrate.
>
> * * *
>
> Hällberg does not explicitly disclose the identification is optically read out of optical-diffraction structures of the optical marking.

The PAN is in machine readable code or magnetic strip, but the secret key number and PIN are not. Hällberg teaches that: "The personal identification number PIN is fed into a register 8 via a customer keyboard 6." Col. 2, line 68 - col. 3, line 2. There is no teaching nor suggestion that the PIN is in a machine-readable or optical read out form. Similarly, there is no teaching nor suggestion that the secret key number is in a machine-readable or optical read out form. Hällberg teaches: "a secret key number K2, which is suitably stored in a RAM memory" and "the key number K1 stored in the memory." Col. 3, lines 29-30 and 59-60.

In contrast, claim 19 encrypts the check number using a machine-readable document number, an identification, which is optically read out of optical-diffraction structures of the optical marking, and a first secret key. Thus, claim 19 requires both a machine-readable document number and an optically read identification as well as a secret key. Hällberg teaches

only one machine readable parameter. Moreover, it would not be obvious to one of ordinary skill in the art to optically read the PIN taught by Hällberg from the card because that would defeat the purpose of a PIN, which is to provide a layer of security that is separate from the information stored on the card or document. One skilled in the art would know this and would not write the PIN on the card/document in any form since it would make the card/document less secure.

Dependent Claims 21-26 Are Not Obvious

For the reasons set forth above, claim 19 is not obvious in view of a combination of Hällberg and Tompkin. These two references neither teach nor suggest producing a check number on a document using a machine readable document number and an optically read identification together with a first secret key. Moreover, theses references neither teach nor suggest authenticating the document by reading the check number from a storage field and performing a cryptographic operation using the machine readable document number and the optically read identification together with a second secret key.

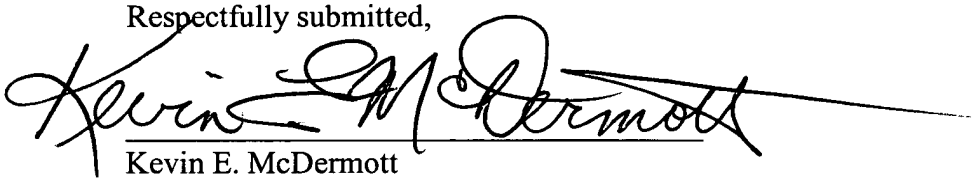
Independent Claims 27 and Dependent Claims 28-36 Are Not Obvious

Claim 27 is a system for activatable documents, which is used to perform the method of claim 19. The system described in claim 27 includes the same limitations as claim 19 and as discussed above, these limitations are not obvious in view of a combination of Hällberg and Tompkin. Accordingly, dependent claims 28-36 are also not obvious.

Conclusion

A combination of the Hällberg patent and the Tompkin et al. patent fails to teach a method of producing and authenticating a check number that uses both a machine readable document number and an optically read identification as required by the claims of the present application. Therefore, the Applicants submit that the claims are not obvious and respectfully request that the Examiner withdraw the rejections based on these references and allow the claims.

Respectfully submitted,



Kevin E. McDermott
Registration No.: 35,946
Attorney for Applicants

HOFFMANN & BARON, LLP
6900 Jericho Turnpike
Syosset, New York 11791
(516) 822-3550
220570_1